

# UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA

**FILED**

**MAGISTRATE JUDGE ASHMAN**

v.

3-12-08

MAR 12 2008 CRIMINAL COMPLAINT

CASE NUMBER:

STEVEN RICHARDSON, and  
KIEWANNA RICHARDSON

MICHAEL W. DOBBINS  
CLERK, U.S. DISTRICT COURT

**08CR**

**210**

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about January 9, 2008, in Cook County, in the Northern District of Illinois, and elsewhere defendants did,

having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, for the purpose of executing the scheme and attempting to do so, knowingly caused to be delivered by Federal Express from St. Louis, Missouri, a package addressed to 7035 South Ashland Avenue, Chicago, Illinois,

in violation of Title 18 United States Code, Sections 1341 and 2.

I further state that I am a(n) Special Agent with the Federal Bureau of Investigation and that this complaint is based on the following facts: See Attached Affidavit

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

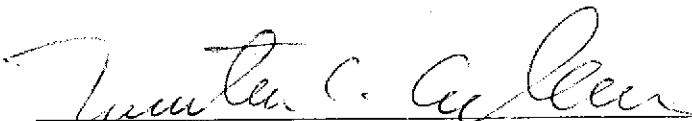
  
Signature of Complainant

Sworn to before me and subscribed in my presence,

March 12, 2008  
Date

at Chicago, Illinois  
City and State

Martin C. Ashman  
U.S. MAGISTRATE JUDGE

  
Signature of Judicial Officer

STATE OF ILLINOIS                     )  
  )       SS  
COUNTY OF COOK                    )

**AFFIDAVIT**

I, BRADLEY J. COLLIGAN, having been duly sworn on oath, state as follows:

1. I am and have been employed as a Special Agent with the Federal Bureau of Investigation ("FBI") since June of 2007. Since June 2007, I have been assigned to the Chicago Field Office of the FBI. As a Special Agent with the FBI, I have investigated violations of criminal law, including those involving bank fraud, identity theft, wire fraud, mail fraud, and conspiracies to commit these violations. Through the FBI, I have received extensive training pertaining to these same violations of criminal law.

2. The information provided below is for the limited purpose of establishing probable cause to believe that KEIWANNA RICHARDSON ("KEIWANNA") and STEVEN RICHARDSON ("STEVEN") knowingly and intentionally devised, participated in, and executed a mail fraud scheme, in violation of Title 18, United States Code, Sections 1341 and 2.

3. This Affidavit is based upon my personal observations, interviews of witnesses, interviews of STEVEN and KIEWANNA, review of documents, reports, as well as information received from other law enforcement agents and investigators. Because of the limited purpose of this Affidavit, it does not contain all information that is known to law enforcement regarding this investigation.

**The Investigation**

4. The Vice-President of Regulatory Affairs and General Counsel for Trinsic Communications ("Trinsic General Counsel"), a company that offers land line telephone service

to its customers, informed your Affiant that multiple customers ("Victims") contacted Trinsic Telecommunications ("Trinsic"), reporting that their credit card account numbers had been used without their authorization. Trinsic General Counsel stated that the Victims reported that the fraudulent use of their credit card numbers had taken place soon after the Victims had provided their credit card numbers over the telephone to a person that the Victims believed worked for Trinsic at telephone number (877) 311-9188. According to Trinsic General Counsel, the Victims stated that they obtained the (877) 311-9188 telephone number to Trinsic by calling directory assistance. Phone calls placed into (877) 311-9188 by the Victims for the purposes of making payments on their Trinsic accounts were first reported on August 16, 2007. The last report of a Victim calling (877) 311-9188 for the purposes of making a payment on his or her Trinsic account was on February 27, 2008. To date, (877) 311-9188 is still an active telephone number and remains in directory assistance as a toll-free telephone number for Trinsic.

5. Trinsic General Counsel informed your Affiant that the (877) 311-9188 telephone number is not a valid telephone number used by Trinsic.

6. According to Trinsic General Counsel, the Victims were calling Trinsic to make bill payments, maintenance requests, and/or change of service requests for which a fee is normally charged. The individuals answering telephone number (877) 311-9188 led the Victims to believe they had contacted Trinsic. According to Trinsic General Counsel, these individuals presented themselves as Trinsic employees over the telephone and obtained the Victims' credit card account numbers and identifying information to pay for the purported Trinsic services.

7. Trinsic General Counsel stated that shortly after calling telephone number (877) 311-9188, the Victims learned that items had been fraudulently purchased on-line using their credit

card numbers. These charges ranged between \$500 to \$2,000.

8. On or about August 16, 2007, the Director of Client Services for Trinsic ("Trinsic Director"), called the aforementioned telephone number and heard a female's voice answer "Trinsic."

9. On or about October 23, 2007, your Affiant contacted the Associate Manager for AT&T Network Fraud Investigations ("AT&T Manager"). AT&T Manager confirmed the manner in which a toll-free number is listed with AT&T toll-free directory assistance. AT&T Manager stated that an individual can contact AT&T and request a toll-free number in the name of any company. AT&T Manager further stated that AT&T confirms this individual to be an authorized representative of the stated company by asking the individual if he or she is an authorized representative. A positive oral response over the telephone allows AT&T to establish a new toll-free number for the stated company as requested by the individual.

10. AT&T Manager told your Affiant that the telephone number (877) 311-9188 was established on or about July 31, 2007 with the number being listed with directory assistance on or about August 6, 2007. AT&T Manager stated further that telephone calls placed to the (877) 311-9188 telephone number were then forwarded to either of two different land-line telephone numbers at 7035 South Ashland Avenue, Basement Apartment, Chicago, Illinois. AT&T Manager stated that the two land-line telephone numbers are (773) 962-9188 and (773) 962-9290. According to AT&T Manager, the telephone numbers are registered to Individual 1, who is listed as a Trinsic Authorized Dealer, 7035 South Ashland Avenue, Basement Apartment, Chicago, Illinois 60636. AT&T Manager also stated that the lines were established on or about July 31, 2007. The number was made available in directory assistance by AT&T on or about August 6, 2007. General

Counsel verified that Individual 1 is not an authorized dealer of Trinsic.

**Telephone Call on October 19, 2007**

11. On October 19, 2007, at 1:17 p.m., an FBI agent acting in an undercover capacity ("UCA") made a consensually monitored and recorded telephone call to the telephone number (877) 311-9188, posing as a Trinsic customer seeking services. UCA used a confidential name for the purposes of the call. After UCA placed the telephone call, a female ("Female Subject") answered the telephone stating, "Trinsic." UCA identified himself using the undercover identity and stated that he needed to make a payment on his Trinsic account. Prior to making the telephone call, UCA was provided with a Trinsic account, which was previously provided to your Affiant by Trinsic for purposes of UCA's telephone call. The Trinsic account had a valid account number and an outstanding balance of \$109.87. The Trinsic account also corresponded to telephone number (850) 944-0575, which was purportedly used by UCA. However, the telephone number was truly a telephone number used by Trinsic Director. UCA referenced the Trinsic account during the call with the Female Subject.

12. After UCA identified himself and his purpose for calling Trinsic, the Female Subject asked UCA for his Social Security Account Number, date of birth, address, telephone number, and outstanding balance on the account. UCA provided this information to the Female Subject. The Female Subject then asked UCA how UCA planned to pay for the balance owed Trinsic. UCA then provided a credit card account number to the Female Subject. The credit card account number used by UCA was a valid Chase Bank Visa card number ("Visa Card"), maintained by law enforcement to facilitate criminal investigations. The Visa Card is maintained in a locked file cabinet within secure FBI space. The Visa Card had not been used in any manner

in over two years and UCA was the only authorized user for this Visa Card. The telephone conversation between UCA and the Female Subject ended at approximately 1:30 p.m. on October 19, 2007.

13. After the telephone call ended, the Visa Card was monitored by Chase Card Services ("Chase") at the request of the FBI. Within a few hours, the FBI was contacted by CHASE and told that a purchase was made on-line using the Visa Card. Chase informed law enforcement agents that the Visa Card was used at 2:16 p.m. on October 19, 2007 to make a purchase with Hewlett-Packard ("HP"), a computer hardware and software store, located in Palo Alto, California. The attempted transaction with HP totaled \$206.94.

14. Law enforcement contacted a Fraud Investigator for HP ("HP Fraud Investigator"), about the purchase made using the Visa Card. HP Fraud Investigator told law enforcement that the transaction was rejected by HP because HP discovered a difference in the billing address for the Visa Card and the billing address provided by the person who used the Visa Card to make a purchase from HP. According to HP Fraud Investigator, the individual who called HP to place the order using the Visa Card provided the name Dantea Kimbrough ("Kimbrough").

15. The billing address for the Visa Card is a confidential address in Chicago, Illinois. However, the address UCA provided to the Female Subject as UCA's address was 707 East Cervantes, Pensacola, Florida 32501 ("Pensacola Address"). According to Fraud Investigator, Kimbrough used the Pensacola Address as her billing address when Kimbrough made the purchase from HP using the Visa Card. According to HP Fraud Investigator, Kimbrough also provided the following information to HP when making the purchase using the Visa Card:

Card Name:	[Confidential Name]
Card Address:	707 E. Cervantes Pensacola, Florida 32501
E-Mail address:	<u>dontekim1985@yahoo.com</u>
Shipping Telephone Number:	(773) 966-5094
Shipping Name:	Dantea Kimbrough
Shipping Address:	7035 S. Ashland Ave., #1 Chicago, Illinois

16. Kimbrough provided 7035 S. Ashland Avenue, #1, Chicago as the shipping address. This is the ground floor apartment just above the basement apartment at 7035 S. Ashland Avenue, Chicago.

17. Shortly after Kimbrough's HP transaction using the Visa Card was blocked due to the differences in billing addresses, Trinsic Director received a telephone call from a Female Subject ("Female Subject 2") claiming to be from "Trinsic."<sup>1</sup> Female Subject 2 asked Trinsic Director for the UCA. Trinsic Director informed Female Subject 2 that UCA was not available, but Trinsic Director offered to take a message for UCA. Female Subject 2 instructed Trinsic Director to inform UCA that the credit card account number that UCA provided Trinsic earlier that day was having problems going through. Female Subject 2 asked Trinsic Director to inform UCA to call Female Subject 2 back at (877) 311-9188 by 8:00 p.m. that night to clear things up. Director informed Female Subject 2 that he would pass along the message to the UCA and ended the telephone call.

---

<sup>1</sup>This telephone call was not recorded. While agents believe that Female Subject 1 and 2 are likely the same individual, voice identifications have not been completed and as a result, the designations in this Affidavit are preliminary.

**HP Records**

18. HP Fraud Investigator informed the FBI that HP identified an additional 52 transactions for the 7035 South Ashland ("Ashland Address") that listed it as the shipping address. HP Fraud Investigator explained that this shipping address was well-known to HP as a source of fraudulent transactions against HP. Fraud Investigator also stated that HP has had several thousand dollars in merchandise shipped to this address for which they were not ultimately paid. HP was not paid due to the credit card transactions being cancelled by their respective banks. The transactions were cancelled after the card holders contacted their banks and informed them they never placed such orders with HP.

19. On or about October 19, 2007, your Affiant reviewed the list provided by HP and determined that there were 52 transactions that occurred between August 29, 2007 to October 19, 2007, all of them using a variation of the Ashland Address. The three different address variations and the number of times that they appear on the list are as follows:

7035 South Ashland Avenue, Chicago, Illinois 60636 (24 times)  
 7035 South Ashland Avenue, Apartment 1, Chicago, Illinois 60636 (20 times)  
 7035 South Ashland Avenue, #1, Chicago, Illinois 60636 (8 times)

20. The transaction that was attempted utilizing UCA's information that was provided to Female Subject is also included in this list. The HP order made using UCA's information was to be shipped the following day.

21. HP Fraud Investigator explained to law enforcement that the orders on the list represented orders placed by individuals using either the Internet or by calling HP's call center. Of the 52 different orders attempted, 12 different names were used. The following is a list of names that were used and how many times each was used in making the HP purchases:

(1) Steven Richardson (5 times used)



- (2) Steve Richardson (7 times used)
- (3) Keiwanna Richardson (1 time used)
- (4) Kiwanna Richards (4 times used)
- (5) Richard Wilson (6 times used)
- (6) Richy Wilson (7 times used)
- (7) Lee Wilson (2 times used)
- (8) Lee Smith (6 times used)
- (9) Dontea Kimbrought (5 times used)
- (10) Dontea Kimbrought (2 times used)
- (11) Danta Kimbrought (5 times used)
- (12) Danta Kimbrought (2 times used)

22. HP Fraud Investigator explained to law enforcement that the individuals placing fraudulent orders frequently try to get the items they ordered shipped for next day delivery, which provides HP with less time to discover the fraud and cancel the transactions.

#### Surveillance

23. Special Agents of the FBI conducted a surveillance of the Residences from October 23rd through October 26th, 2007. On Friday, October 26, 2007, your Affiant witnessed a Federal Express ("FedEx") delivery person walk up to the Residences. The FedEx employee appeared to push one of the two doorbells on the outside of the front door of the Residences. Shortly afterward, the window on the first floor was opened by a female ("Female Subject 3") inside. The FedEx employee handed what appeared to be a clipboard through the opened first floor window to Female Subject 3 inside. Female Subject 3 was seen through the window on the first floor of the residence. Female Subject 3 received the item and soon thereafter handed it back to the FedEx employee. The FedEx employee then picked up the package and handed it to Female Subject 3 inside through the open window. The FedEx employee then walked back to the FedEx truck and

drove away.<sup>2</sup>

24. An Investigator for FedEx ("FedEx Investigator"), was contacted about the package that was delivered to the Residence on October 26, 2007. FedEx Investigator said the package had a shipping address listed as Monique Wilson, 7035 South Ashland Avenue, Chicago, Illinois, 60636. Upon delivery, FedEx Investigator said the package was signed for as "M. Wilson." The package had a return address listed as Michael Jacobs, MKM/Charming Shoppes, 8256 Zionsville Road, Indianapolis, Indiana 46268.

25. A Fraud Prevention Manager for Charming Shoppes, Inc. ("CSI Fraud Prevention Manager"), was contacted about the package delivered to Monique Wilson at the Residence on October 26, 2007 from Charming Shoppes, Inc. ("CSI") said that the shipping address sounded familiar and that he would check on it. CSI Fraud Prevention Manager checked his computer and responded that Fashion Bug, a company under CSI, did have an order that was shipped out to Monique Wilson at this 7035 South Ashland Avenue address on October 26, 2007.

26. CSI Fraud Prevention Manager provided the following information about the purchase.

Order Number:	83492601
Shipping Recipient:	Monique Wilson
Shipping Address:	7035 South Ashland Avenue Chicago, Illinois 60636
Items Ordered:	(6) pairs of L.A. Blues jeans (Size 30W) (1) pair of Gitano jeans (Size 32 W) (2) pairs of Zana Di jeans (Size 32W)
Order Price:	\$285.54

---

<sup>2</sup>While surveillance agents were unable to positively identify Female Subject 3, according to FedEx records, the package was signed for using an alias commonly used by KIEWANNA.

27. CSI Fraud Prevention Manager said that the order was originally placed on or about October 19, 2007. Due to problems CSI had with this shipping address in the past, a hold was placed on the order so that CSI fraud prevention employees could review it. A call was placed to (773) 307-9474 by fraud prevention employees for CSI to verify the billing address, but nobody was reached. CSI Fraud Prevention Manager stated that a woman claiming to be the victim card holder returned the telephone call from (773) 307-9474 on or about October 25, 2007 and said that she authorized the transaction to take place. After this telephone call, CSI allowed for the transaction to process and sent the items to the aforementioned shipping address via FedEx for delivery on the next day.

28. CSI Fraud Prevention Manager said that they have had numerous transactions or transaction attempts involving this shipping address of 7035 South Ashland Avenue, Chicago, Illinois. He said that CSI was able to cancel some of the transactions before the items were shipped out due to discrepancies with the billing addresses, telephone numbers provided, and shipping addresses.

29. CSI Fraud Prevention Manager said that Fashion Bug was paid by Visa for the fraudulent transaction that processed on October 25, 2007, but he expects that Visa will probably reverse the charges due to a "charge back dispute" from the victim card holder.

#### **Memory Giant Transaction**

30. Special Agents of the FBI conducted an investigation based on a package that was delivered to 7035 South Ashland, Chicago, Illinois on January 9, 2008 by FedEx. This shipment was ordered from Memory Giant located at 655 Leffingwell Avenue, St. Louis, Missouri. A customer service representative for Memory Giant ( "MG Customer Service Representative")

received an order for Random Access Memory ("RAM") for a Dell computer totaling \$178.98. The credit card account number provided for payment by the caller was a Mastercard account ending in 7527. The credit card account billing information provided was for Victim 1. The shipping address provided for delivery was 7035 South Ashland Avenue, Chicago, Illinois. The recipient name provided was RICHY WILSON. The telephone number provided was (312)659-0909. The FedEx tracking number assigned to this delivery was 798847164079. The order was shipped priority overnight delivery. Memory Gian did not receive payment for this order. MG Customer Service Representative stated that it was a charge back to Memory Giant because the credit card used for the order was reported stolen.

#### **Search Warrant**

31. A search warrant was executed at the residence located at 7035 South Ashland Avenue, Chicago, Illinois on March 11, 2008. Among the items that were seized during the search were multiple sheets of paper with type written information, including names, dates of birth, social security account numbers, addresses, credit card account numbers, and credit card expiration dates. This information related to people from various places throughout the United States, such as Massachusetts and New York. Also seized were numerous cellular telephones and computers. Law enforcement also seized various packaging materials.

#### **Interview of STEVEN and KEIWANNA**

32. On March 11, 2008, STEVEN and KEIWANNA were separately interviewed by law enforcement in connection with the fraud scheme. After separately being provided with their *Miranda* warnings, STEVEN and KEIWANNA agreed to speak with law enforcement. STEVEN and KEIWANNA each admitted to participating in a fraud scheme with one another and

Individual 2. More specifically, STEVEN and KEIWANNA stated that they set up various toll-free telephone numbers through AT&T by falsely stating that they were representatives of various businesses, including Trinsic. They stated that they would get these telephone numbers listed on directory assistance. STEVEN and KEIWANNA stated that using this procedure, STEVEN, KEIWANNA and Individual 2 posed as representatives for Sprint, Trinsic, and Comcast.

33. STEVEN stated that he set up the Trinsic telephone number with AT&T. STEVEN stated that he set up the telephone numbers in order to fraudulently obtain the names and credit card account information of actual customers of this company. KEIWANNA stated that she set up the Comcast telephone number with AT&T. KEIWANNA established this telephone number in order to fraudulently obtain the names and credit card account information of actual customers of the company.

34. STEVEN and KEIWANNA further stated that STEVEN, KEIWANNA and Individual 2 would then take turns answering the telephones in the basement of 7035 South Ashland Avenue, Chicago, Illinois, pretending to be the customer service representatives of the companies. STEVEN and KEIWANNA stated that Victims would call in and after being prompted by STEVEN, KEIWANNA or Individual 2, the Victims would provide their names, credit card account numbers, dates of birth, social security account numbers and addresses. STEVEN and KEIWANNA stated that STEVEN, KEIWANNA and Individual 2 would use the Victims' information to make online purchases for electronics, and clothing.

35. STEVEN and KEIWANNA further stated that STEVEN, KEIWANNA and Individual 2 received approximately 50 telephone calls per day using this scheme, but would only answer approximately 20 of the calls. STEVEN and KEIWANNA stated that STEVEN,

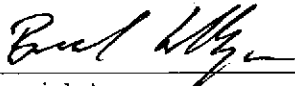
KEIWANNA and Individual 2 would then use the credit card account information that they obtained from the customers to purchase as much as possible on each credit card account that they could, up to the limits of the cards. While conducting the scheme, STEVEN and KEIWANNA stated that STEVEN, KEIWANNA and Individual 2 fraudulently purchased merchandise online using this credit card information. KIEWANNA and STEVEN stated that the online stores that STEVEN, KIEWANNA, and Individual 2 made purchases from include Hewlett-Packard, Best Buy, Dell, Old Navy, and Toys-R-Us. STEVEN stated that he also purchased merchandise online from Memory Giant, Verizon Wireless, Staples, and US Cellular. KEIWANNA stated that she also purchased merchandise online from Fashion Bug and Just My Size.

36. STEVEN further stated that on January 8, 2008, he placed an on-line order with Memory Giant for Random Access Memory (RAM) using an alias, Richy Wilson. Richardson purchased the RAM for \$178.98 by using a credit card account number that did not belong to him. The RAM was sent and delivered via FedEx to STEVEN at 7035 South Ashland Avenue, Chicago, Illinois on January 9, 2008. The package was signed for by Richy Wilson, which STEVEN stated is an alias that he commonly uses. Memory Giant did not receive any payment for this order.

CONCLUSION

37. Based upon the foregoing paragraphs, I believe that there is probable cause to believe that KIEWANNA RICHARDSON and STEVEN RICHARDSON knowingly and intentionally devised and participated in a scheme to defraud that was executed by mail in violation of Title 18, United States Code, Section 1341.

FURTHER AFFIANT SAYETH NOT

  
Special Agent  
Bradley J. Colligan  
Federal Bureau of Investigation

Sworn and subscribed to before me, this 12th Day of March, 2008

  
MARTIN C. ASHMAN  
UNITED STATES MAGISTRATE JUDGE